Abstract

Scalable and unified multipliers for multiplication of cryptographic parameters represented as elements of either of the prime field ($GF(p)$) and the binary extension field ($GF(2^m)$) include processing elements arranged to execute in pipeline stages. The processing elements are configurable to perform operations corresponding to either the prime field or the binary extension field. In an example, the processing elements include a dual-field adder having a field-select input that permits selection of a field arithmetic. In a representative example, multipliers are implemented as integrated circuits having processing units that each receive a single bit of one operand and partial words of the remaining operand.